

Account Management Policy



The Thabachweu Local Municipality policies are statements of principles and practices dealing with the ongoing management and administration of the Municipality's IT assets. These policies act as a guiding frame of reference for how the Municipality deals with everything from its day- to-day IT operational and support procedures to comply with security regulations and codes of practice. This "statement of purpose" will guide the actions to be taken to achieve that purpose.



Thabachweu Local Municipality

Table of Contents

1. Overview.....	2
2. Purpose.....	2
3. Scope	2
3.1. Access controls	2
3.1. User Account	3
3.2. Computer Account.....	4
3.3. Service account.....	4
3.4. Account management	4
3.5. Password reset	5
3.6. Decommission process	6
3.7. Exceptions.....	6
3.8. Responsibilities	6
4. Corrective actions for non-policy compliance	7
5. Glossary and Abbreviations	7
Version Control.....	8
Author.....	8
Review	8
Approval	8



Thabachweu Local Municipality

1. Overview

Effective security controls in relation to access to data are an essential component of the effective risk management of the Municipality. User accounts offer a way of managing access, providing user accountability and tracking their use of information, information systems and resources. User accounts can take various Forms from a system login to an ID access card. Therefore the application of access controls, the management of user accounts and the monitoring of their use plays an extremely important part in the overall security of information resources.

2. Purpose

The purpose of the account management policy is to establish the rules for creating and administering user and computer accounts of the Thabachweu Local Municipality. An account, at minimum, consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources. This policy establishes standards for issuing accounts, creating password values, and managing accounts.

3. Scope

3.1. Access controls

- Access controls will be established for all major information, information systems and facilities based on their classification and security risk assessment to ensure that the appropriate level of security is implemented;
- Logical access controls will be implemented in accordance with this policy and the Information Security Policy. Physical access controls will be implemented in line with this policy and the Physical and environmental Security Policy;
- Access to the network, information systems and servers will be achieved by the use individual user accounts (UIDS) that will require an appropriate authentication method as outlined in the Password and Authentication Policy;
- Access to information systems and facilities will be governed by a formally defined authorisation process covering the creation, modification/maintenance, re-enabling and deletion of accounts;
- Users will only be granted access to information and information systems and facilities on a “need-to-know” basis. Users will only be granted the minimum access and privileges required to perform their duties;
- Procedures will be implemented to ensure that access to data or information is not dependant on any one individual. Privileges granted by groups will be implemented in order to facilitate this function;



Thabachweu Local Municipality

- Each assigned account will uniquely identify the user and must conform to the Council's naming standard (making use of the users name/surname) or an appropriate coding structure. Accounts must not give any indication of the user's access rights;
- Security of systems administration accounts and passwords will be the responsibility of the technical owner of that system and must adhere to the Council policies with the exception of where this is not technically possible;
- A notice warning users about accessing information without authorisation will be displayed before users can gain access to any information system or facility. It should not identify any information about the information system or any other internal matters;
- A review period, determined by the information "owner", will be established to reassess the access controls implemented for information, information systems and facilities. A record of the review must be maintained;
- User accounts will be reviewed on a regular basis to ensure access and account privileges remain applicable to the job function/role or employment status of the user. A record of the review must be maintained;
- All employees have a legal duty to keep all personal data confidential and to comply with the data protection provisions contained within the Code of Conduct for Employees;
- Access to information systems and facilities will be revoked for users who do not need access to perform their duties in order to ensure the confidentiality, integrity and availability of information to other users.

3.1. User Account

In Active Directory, a user account is an object that consists of all the information that defines a domain user, which includes user name, password, and groups in which the user account has membership. User accounts can be stored in either Active Directory or on your local computer.

The following process must be followed when a new user account is created for a new user on the Municipality's infrastructure.

- The Municipality's "user account creation" form should be completed with all the required user information; the IT infrastructure required and the services required such as e-mail and internet.
 - Document to be completed: Thabaform_User Account_v1.1.pdf
- The account must be created in the correct OU in the Active Directory User and Computers applet.
- When a user account is created in the Microsoft Active Directory Service the default password: **Password1** will be used and the user will be prompted to change the password on first logon.
- When establishing accounts, standard security principles of "least required access" to perform a function must always be used, where administratively feasible. For example, a root or administrative privileged account must not be used when a non-privileged account will do.



Thabachweu Local Municipality

- All accounts shall be reviewed at least annually by the Municipality's Security Officer to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status.

3.2. Computer Account

A computer account is an account that is stored in Active Directory and that uniquely identifies a computer in the domain. Computer accounts are created for any computer running Windows NT, Windows 2000, Windows XP Professional or Windows Server 2003 that joins the domain. They are managed through Active Directory Users and Computers applet.

The following process must be followed when a computer joins the domain and the computer account is created.

- One of the Municipality's IT support personnel joins the computer to the domain by using the "join computer to the domain" service account – ThabaJoin.
- The Windows Deployment Services was used to re-load the computers operating system and software applications. During the Operating system install process it join the computer in a secure manner to the Thabachweu.local domain. This process uses the "join computer to the domain" service account – ThabaJoin.
- During the Windows Deployment Process computers are joined to the ThabaComputers OU in the root tier of the Thabachweu.local domain and that is where the computer account will reside.
- The computer account will be created in the default "Computers" OU in the root tier of the Thabachweu.local domain. The computer account must be moved manually to the ThabaComputers OU.
- All the Municipality's computer accounts will reside in the ThabaComputer OU for GPO assignments.

3.3. Service account

User accounts can also be used as dedicated service accounts for some applications. A dedicated service is a program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level. The following user accounts are used as service accounts:

- ThabaJoin Standard User Used for joining computers to the domain.
- ThabaBackup Domain Administrator Used for backup services.

3.4. Account management

- Accounts will only be created and maintained for users that need access to information, systems and facilities to perform their official duties on behalf of the Council;



Thabachweu Local Municipality

- User accounts will only be authorised to the capabilities appropriate to the user's role requirements, responsibilities or specific needs to carry out a function for which they are employed. Users will only be assigned the access privileges needed to carry out their job function.
- All accounts created or modified must have a documented request and the appropriate authorisation. A record must be maintained of all authorisations including the access rights and privileges granted;
- Procedures will be established to ensure user's access rights and privileges are adjusted in a timely manner whenever there is a change in a user's status;
- User accounts will not be activated until the authorisation process has been correctly completed. Users must not have access to information systems until all activities relating to the commencement or resumption of employment have been completed i.e. acknowledgement of Acceptable Use Policy;
- Generic or shared accounts will not be permitted. The only exception will apply to mail accounts required by services where Information & Data Management Section has granted approval;
- Upon notification of termination, transfer, resignation, suspension or retirement from employment received from the relevant authoritative source(s) the user account will be disabled. Each user account must be unique, only connected with the user to whom it was originally assigned. Reuse of user IDs is not permitted;
- All user accounts will as a minimum force the use of a password;
- All default passwords for accounts must be constructed in accordance with the Council's Password & Authentication Policy. All default passwords must be immediately changed by the user immediately after logging into the system if not prompted automatically to do so;
- User accounts with system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by the user.

3.5. Password reset

The following procedure must be adhered to for user account password reset:

- The identity of users must be authenticated before a password will be reset.
- The default "Password1" will be used for all user account password resets. The user will be requested to change the password on the first successful logon to the Thabachweu.local domain.
- Whenever possible, passkeys should be used to authenticate a user when resetting a password or activating a guest account, and should comply with the above standards. Passkeys provide one-time access to a system or application and require the user to change to a password of their choice upon initial login. Where passkeys are not feasible, pre-expired passwords should be used.
- Automated password resets are available and may be utilized, provided that a recognized and approved method is used (e.g. Gartner recommended), such as multiple, random challenge and response questions.
- Passwords must be reset over an encrypted tunnel (SSL, ssh, or VPN, for example).
- Password change events should be recorded in an audit log.



Thabachweu Local Municipality

3.6. Decommission process

Only the Municipality's Security Officer can approve the decommission process for inactive user or computer accounts.

- Computer accounts scheduled for the decommissioning process must be disabled and moved to the "Graveyard" OU. These accounts will only be deleted at the end of each month.
- User accounts scheduled for the decommissioning process must be disabled and moved to the "Graveyard" OU. These accounts will not be deleted and will remain as a reference security account for 5 year.
- Only domain administrators are allowed to manage and administer user and computer accounts in the Municipality's Active Directory Services.

3.7. Exceptions

- Exceptions to this policy will only be granted if:
 - Compliance would adversely affect the ability of the service to accomplish a mission critical function; or
 - Compliance would have an adverse impact on the service provided or supported by the information, system or resource; or
 - Compliance cannot be achieved due the incapability of the information system or resource.
 - A procedure for requests for exception to this policy will be produced and implemented

3.8. Responsibilities

- Human Resources are responsible for:
 - Ensuring that information held within the HR system is accurate and kept up to date
 - Providing all employees with a copy of the Acceptable Use policy ensuring it is acknowledged/signed by the employee;
- System administrators/security officers, as custodians, are responsible for:
 - The creation, modification and deletion the user accounts relating to their information system(s):
 - Ensuring processes associated with the creation, modification and deletion of accounts are documented in formal procedures.
 - Periodical review of users accounts for validity
 - Monitoring user account activities and reporting unusual activities to management
 - Providing a list of inactive accounts to HR in order that the status of the account/account holder can be verified;
 - Co-operating with authorised Council personnel in the investigation of security incidents in line with the Incident Management Policy
- Line Managers are responsible for:



Thabachweu Local Municipality

- Promptly notifying HR when permanent and temporary employees, contractors and service partner personnel terminate employment or transfer to new duties/responsibilities;
- Promptly notifying the relevant systems administrators when staff, contractors and service partner personnel terminate employment or transfer to new duties/responsibilities;
- Providing all temporary employees employed within their service with a copy of the Acceptable Use Policy ensuring it is acknowledged/signed for by the individual.
- All Users are responsible for:
 - Familiarising themselves with this policy and all other related policies and guidelines set out below;
 - All activity related to accounts they have been allocated.
 - Reporting any suspected misuse of accounts/passwords to their line manager.
 - Ensuring the security of their own passwords and reporting any potential compromise to the security of their user accounts.
- Information & Data Compliance is responsible for:
 - Maintaining this policy;
 - Ensuring processes associated with the above are documented in formal procedures.

4. Corrective actions for non-policy compliance

- Failure to comply with the guidelines stipulated in the Municipality's policies will result in the following corrective or disciplinary procedures.
- The decisive action that will be taken against the employee is dependent on the severity level and the level of the security risk.
- Warning from Management
 - The employee receives a warning from their manager that they were in violation of policy.
- Written Warning in Personnel File
 - The employee is reprimanded, and official notice is put in their personnel file. This may have negative consequences during future performance reviews or promotion considerations.
- Revoking Privileges
 - Access to certain resources, such as internet or email, can be revoked for a limited period providing that this action does not have a negative impact on the employee's job functions.
- Training
 - Adequate training to create awareness and guidance on policy compliance.
- Disciplinary action will be determined in compliance to Schedule 8 of the Labour Relations Act 66 of 1995 or other related Public Service Regulations.

5. Glossary and Abbreviations

Please refer to the Thabachweu Glossary and abbreviations guide.



Thabachweu Local Municipality

Version Control

Version	State/Change	Author	Date
1.0	Original	Sbusiso Langa	
1.1	Changes	Sbusiso Langa	

Author

Name	Designation	Signature	Contact
Sbusiso Langa	Security Officer		+27 13 235 7367

Review

Name	Designation	signature	Date

Approval

Name	Designation	Signature	Date